IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. TAUREAN JEROME WEBER, Defendant.	CR 21–28–M–DLC ORDER

Before the Court is the United States' Motion in Limine for Pretrial Determination of Admissibility of Certain Business Records. (Doc. 30.) The United States moves this Court in limine for an order holding that various records from Charter, Google, Facebook, and Dropbox are self-authenticating and a record's custodian need not testify at trial regarding the authenticity of such records. (Doc. 31 at 1–2.) Defendant Taurean Jerome Weber objects. (Doc. 34.) For the reasons stated herein, the Court will deny the motion.

ANALYSIS

Motions in limine are a "procedural mechanism" through which questions regarding the admissibility of "testimony or evidence in a particular area" may be resolved before trial. *United States v. Heller*, 551 F.3d 1108, 1111 (9th Cir. 2009). Such in limine rulings really are just preliminary, and the Court "may always

change [its] mind during the course of a trial." *Ohler v. United States*, 529 U.S. 753, 758 n.3 (2000). With this in mind, the Court will turn its attention to the merits of the underlying motion.

Mr. Weber is charged by indictment with several child pornography related offenses. (Doc. 2.) At trial, the United States intends to offer evidence consisting of "records and data from several accounts associated with, created by, and used by" Mr. Weber. (Doc. 31 at 2.) This appears to include the substantive content of such accounts including "sexually explicit material," internal messages, and the underlying CyberTips and associated attachments sent by Instagram to the National Center for Missing and Exploited Children. (*Id.* at 4–6.)

Through its motion, the United States seeks an in limine ruling that such evidentiary items are self-authenticating, or "prima facie authentic," so that it may admit them at trial "without foundation testimony from the records custodian or other qualified witness." (*Id.* at 4, 6.)[1] The United States' couches its motion under Federal Rules of Evidence 803(6), 902(11), and 902(13) (*Id.* at 6–7) and provides examples of certifications through which it intends to admit the subject evidence (Doc. 31-1).

The Court beings with Rule 803(6), which, through explicit textual

[1] The United States recognizes that the admission of such evidence could still be challenged at trial based on other evidentiary considerations such as relevancy. (*Id.* at 3–4.)

connection, operates in tandem with Rule 902(11). *United States v. Kahre*, 610 F. Supp. 2d 1261, 1263 (D. Nev. 2009). This rule exempts evidence from the exclusionary consequence of the general hearsay rule if it constitutes:

> record of an act, event, condition, opinion, or diagnosis if the record was made at or near the time by—or from information transmitted by—someone with knowledge, the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit, making the record was a regular practice of that activity, all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) . . . and the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

Fed. R. Evid. 803(6). This provision is generally referred to as the business records exception. *U-Haul Intern, Inc. v. Lumbermens Mut Cas. Co.*, 576 F.3d 1040, 1044 (9th Cir. 2009).

Rule 902(11) complements Rule 803(6) by providing a mechanism through which business records can be authenticated short of live foundational testimony. *Kahre*, 610 F. Supp. 2d at 1263. Unsurprisingly, evidence must be authentic to be admissible. *Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 (9th Cir. 2002) (citing Fed. R. Evid. 901(a)) ("Authentication is a 'condition precedent to admissibility'"). In general, to be authenticated, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). But this need not be done for certain categories of so-called "self-authenticating" evidence, *United States v. Weiland*, 420 F.3d 1062,

1071 (9th Cir. 2005), which are enumerated in Federal Rule of Evidence 902.

Rule 902(11) establishes an authentication "exception for certified domestic records of regularly conducted activity." *Id.* at 1072. This rule provides:

> The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record--and must make the record and certification available for inspection--so that the party has a fair opportunity to challenge them.

Fed. R. Evid. 902(11). Under Rule 902(11) then, certified business records are self-authenticating. The requisite certification may be accomplished through a declaration satisfying the requirements of 28 U.S.C. § 1746, or any other "comparable certification under oath." Fed. R. Evid. 902(11), Advisory Committee Note—2000 Amendment.

Mr. Weber argues the evidentiary items at issue are not business records and therefore are not self-authenticating pursuant to Rule 902(11). (Doc. 34 at 3–7.) The focus of his argument is on the "substantive content" of the evidence, including images, videos, or messages on his social media accounts. (*Id.*) In support, Mr. Weber cites to the Third Circuit's decision in *United States v. Browne*, 834 F.3d 403 (3d Cir. 2016). In *Browne*, the defendant "was convicted of child pornography and sexual offenses with minors based in part on records of 'chats' exchanged over Facebook and [] contest[ed] his conviction on the ground

that these records were not properly authenticated with evidence of his authorship." 834 F.3d at 405.

On appeal, the Third Circuit rejected the government's argument that such "Facebook chat logs" are self-authenticating pursuant to Rule 902(11). *Id.* at 409. Its analysis was two-fold. First, the Third Circuit concluded that the Rule 902(11) certification provided in the case was insufficient to establish that "Browne and the victims authored the Facebook messages at issue." *Id.* at 410. Because "the relevance of the Facebook records hinges on the fact of authorship," the Third Circuit concluded that the government had failed to sufficiently "fulfill[] its authentication obligation simply by submitting" a certification that "communications took place as alleged between the named Facebook accounts." *Id.*

Second, because "[a]t most, the records custodian employed by the social media platform can attest . . . that the depicted communications took place between certain Facebook accounts, on particular dates, or at particular times," the substantive content of the message remained unauthenticated. *Id.* at 410–11. Therefore, because "the Government's interest lies in establishing the admissibility of the chat logs in full," they were not "business records under Rule 803(6) and thus cannot be authenticated by way of Rule 902(11)." *Id.* at 411.

This approach is consistent with the results of other Circuit Courts of Appeal

that have addressed the issue. *United States v. Lewisbey*, 843 F.3d 653, (7th Cir. 2016) (holding that in order to authenticate social media posts, the government must introduce some sort of extrinsic evidence that the account belongs to the defendant); *United States v. Barber*, 937 F.3d 965 (7th Cir. 2019) ("To authenticate Facebook records and messages, the government" must "produce evidence sufficient to support a finding that the account belonged to Barber and the linked messages were actually sent and received by him"); *United States v. Lamm*, 5 F.4th 942, 948 (8th Cir. 2021) (holding that in child pornography prosecution "the Government may authenticate social media evidence with circumstantial evidence linking the defendant to the social media account"). In the absence of directly controlling Ninth Circuit precedent, the Court will chart a similar path to that forged by the Third, Seventh, and Eighth Circuits regarding the authentication of records from online accounts.

First, the Court does not find that the entirety of the electronic records at issue are business records within the meaning of Rule 803(6). In the Ninth Circuit, a record is not "kept in the course of a regularly conducted activity of a business," as required for application of Rule 803(6), unless it is "made pursuant to established company procedures for the systematic or routine and timely making and preserving of company records." *Clark v. City of L.A.*, 650 F.2d 1033, 1037 (9th Cir. 1981). The record must also be "relied upon by the business in the

performance of its functions." *Id.* (adding the "basis for the business record exception is that accuracy is assured because the maker of the record relies on the record in the ordinary course of business activities"). This understanding of the business records exception governed the Third Circuit's analysis in *Browne*, 834 F.3d at 409–10, and does so here as well.

To the extent the United States argues that the substantive content of the Charter, Google, Facebook, and Dropbox accounts at issue in this case are business records, the Court disagrees. Nothing in the record establishes that Charter, Google, Facebook, and Dropbox "verify[s] or rel[ies] on the substantive content" of the accounts at issue in the course of its business. *Id.* at 410. The substantive content of the accounts at issue, such as messages, images, videos, were not made, nor relied on, by the providers for the purpose of conducting their respective businesses. *Clark*, 650 F.2d at 1037. As such, the Court concludes the substantive content of the records at issue are not self-authenticating business records under Rule 902(11). *Browne*, 834 F.3d at 411.

As Mr. Weber recognizes, perhaps certain "technical" aspects of the records at issue could constitute business records capable of authentication under Rule 902(11). (Doc. 34 at 6.) This might include "timestamps on . . . chats, the fact that chats took place between particular . . . accounts," or other similar information. *Browne*, 834 F.3d at 411. Because the Court has not actually reviewed the

evidence, nor has the United States sought such piecemeal authentication, the Court will not enter a preliminary ruling authenticating any of the evidence at issue pursuant to Rule 902(11). *Id.*

The United States alternatively argues the evidence is self-authenticating under Rule 902(13). Rule 902(13) provides render self-authenticating certified records generated by an electronic process or system. This rule provides in full:

> A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

Fed. R. Evid. 902(13). The United States' reliance on this evidentiary provision is similarly unavailing.

Rule 902(13), by its very terms, applies only to records created via an electronic process. It does not render self-authenticating substantive content created, shared, or stored, by a user of a social media account. Wright and Miller § 7147 ("It is important to note that" Rule 902(13) "does not include records created by a human that are stored in an electronic format"). Such content arises not from an automatic electronic process but from the actions of the user of the account. This is not the sort of evidence generated by electronic process that falls within the scope of Rule 902(13). *Western Towboat Co. v. Vigor Marine, LLC*, 2021 WL 2641521, *4–5 (W.D. Wash. 2021) ("archival weather data" collected

automatically by a website is Rule 902(13) evidence); Wright and Miller § 7147 (providing four examples of Rule 902(13) evidence including: (1) information automatically recorded in the registry of a Windows operating system; (2) information within a server's "Internet information Services (IIS) log;" (3) photo metadata automatically generated by iPhone software; and (4) text log information that is automatically generated such as "the date and time of each text and the number of the other phone").[2] Because the evidence at issue certainly encompasses the substantive content of certain electronic accounts not generated by electronic processes, the Court cannot hold that it is self-authenticating under Rule 902(13).

Accordingly, IT IS ORDERED that the motion (Doc. 30) is DENIED.

DATED this 6th day of December, 2021.

Dana L. Christensen, District Judge
United States District Court

[2] Notably, Wright and Miller specifically states that, as to this fourth category, Rule 902(13) would not "authorize the introduction of the content of the text messages." *Id.*